DIGITALEUROPE

4 JUNE 2025

Digital simplification package: Our data recommendations

Europe's ambition to shape a single market for data is not in question. But the complex legislative path we've taken threatens the very goals it set out to achieve. The Data Act, in particular, is underpinned by a sweeping, untested assumption: that companies are dominant in their markets, are hoarding data and must therefore be compelled by law to share it.[1] It applies the same rules to all products, regardless of market structure, and regardless of whether the product is already part of a flourishing ecosystem or a stagnant silo.[2]

In addition, the Data Act prevents companies from using data unless they first renegotiate mandatory contractual terms.[3] As of September 2025, data holders may lose the ability to process such data unless they amend existing contracts with users. This requirement applies regardless of whether the users are businesses or individuals, creating a heavy operational burden.

This logic criminalises data markets before they've even had a chance to develop, and hurts the competitiveness of our most promising digital and digitalising businesses.

In this paper, we detail changes that are necessary to remedy these fundamental flaws. As Europe prepares to discuss these changes in the upcoming digital package, we urge for an **immediate postponement of at least one year of the Data Act's entry into application**.[4]

---

[1] Regulation (EU) 2023/2854.

[2] The decision to impose across-the-board data-sharing obligations rested on a fragile evidentiary foundation. One of the central studies cited in the Data Act impact assessment explicitly acknowledged the profound limits of its findings. The study observed that the data economy remains in the 'emergence phase' of market development, with most European businesses still evaluating how to integrate new technologies into their business models. As the authors candidly noted, 'the small number of cases and the difficulty for the companies themselves of knowing the true scale or cost of barriers that are still emerging put limits on meaningful quantification.' See *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*, prepared by Deloitte for the European Commission, available at https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en.

[3] Arts 4(12)-(13) Data Act.

[4] A similar approach was recently adopted for the sustainability omnibus package, which included a 'stop-the-clock' proposal (promptly adopted as Directive (EU) 2025/794) delaying reporting obligations. The delay is intended to prevent an abrupt compliance cliff for companies whilst changes to Europe's sustainability framework are being discussed.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

Table of contents

Make data sharing voluntary by default

- Make data sharing under the Data Act voluntary by default, supporting Europe's industrial innovation.
- Empower the Commission to recognise industry-developed codes of conduct, allowing tailored data-sharing frameworks for different types of connected devices.

The Data Act's original design can be reconciled with a **voluntary framework**.

Where there is no demonstrated problem, data sharing should not be imposed. The Act should serve as a ready-to-use governance framework that companies can adopt to structure data-sharing arrangements in a transparent, secure and fair way. It offers a model for enabling user access and third-party sharing, supported by trade secret protections, cybersecurity safeguards and fair compensation rules.

This voluntary approach gives companies operating connected devices the flexibility to organise data access in a way that supports existing practices whilst encouraging innovation and trust. Businesses that choose to align with the Data Act's principles can demonstrate their commitment to fair and responsible data sharing.

To support this model, the Commission should be empowered to **recognise industry-developed codes of conduct**. These codes would allow different categories of connected devices to tailor their data-sharing

frameworks whilst ensuring alignment with the Data Act's objectives. Such recognition would promote good practice and reinforce trust in the market.[5]

This approach preserves the political balance achieved in the original legislation. It allows the framework to evolve gradually, guided by real-world developments, and provides predictability for companies that have been adapting to the current rules.

Strengthen trade secrets and cybersecurity protections

- Recognise trade secrets and cybersecurity as fully legitimate grounds to withhold data under the Data Act, without triggering mandatory notifications.
- Shift the burden of contesting refusals to the requester, rather than the data holder.

The Data Act establishes certain safeguards for data holders – including protection of trade secrets and cybersecurity risks – when assessing data sharing requests. However, these defences are framed too strictly, and place an excessive procedural burden on the data holder.

Arts 4(6)–(8) establish procedures for withholding or refusing data sharing in cases involving trade secrets. In both cases, the data holder must not only substantiate its decision extensively with evidence of *serious* economic harm, but also notify the competent authority. This mandatory notification suggests that any refusal to share data, even when justified by serious economic risks, is treated as an exception requiring oversight, rather than as a normal exercise of entrepreneurial discretion to protect critical assets.

Similarly, Art. 6(2)(f) merely stipulates a generic requirement for third parties not to use the data they receive 'in a manner that has an adverse impact' on security. Art. 4(2) allows the data holder to restrict or prohibit data sharing only for security risks that could result in 'serious adverse effect.' As with trade secrets, the onus is fully on data holders to notify the competent authority, reinforcing a presumption that the invocation of legitimate defences is exceptional and abusive.

Protections such as trade secrets and cybersecurity should be treated as fully recognised legal grounds to withhold access, without triggering automatic scrutiny. Rather than mandating notification to authorities, the mechanism should be reversed: users who consider a refusal unjustified should have the possibility to challenge the decision before the independent dispute settlement bodies established under

[5] The Commission's power to recognise industry codes of conduct or equivalent instruments has several precedents in EU legislation. For example, Art. 40 GDPR allows associations and other bodies to prepare codes of conduct intended to contribute to proper application of the Regulation, which can be approved by data protection authorities and ultimately recognised by the Commission. Similarly, under Art. 45 of the Digital Services Act (Regulation (EU) 2022/2065), the Commission may encourage and assess codes of conduct covering specific areas such as online advertising and protection of minors. The Unfair Commercial Practices Directive (Directive 2005/29/EC) also provides for the recognition of codes of conduct to help ensure compliance with fair trading standards. These precedents demonstrate that recognition of voluntary frameworks can support legal certainty and foster good practice, without imposing rigid new obligations.

Art. 10, or before the courts. This would ensure that legitimate refusals are not systematically discouraged and that oversight is reserved for genuine disputes, not every exercise of risk management.[6]

Clarify temporal scope

- Amend the Data Act's definition of 'placing on the market' to exclude legacy products, developed years ago but placed on the market over long delivery timelines (e.g. vehicles, aircraft).
- Apply data sharing obligations only to future contracts, preventing disproportionate retroactive effects.

Even if the Data Act is revised to operate on a voluntary-by-default basis, it remains critical to clarify key provisions governing its scope and temporal application. In particular, the provisions on the placement of products on the market and the validity of existing contracts must be revised to avoid disproportionate retroactive effects.

First, the **definition of 'placement on the market'** under Art. 2(22) must be amended to **ensure that legacy product types** – including those developed and certified years in advance, but placed on the market over long delivery timelines – are **not unintentionally brought into scope**. This is essential in sectors such as automotive, medical technology or aerospace, where the product lifecycle from design to deployment spans multiple years. Without clarification, the Data Act could delay or disrupt market access for essential industrial systems.

Second, **Art. 50 should be amended to ensure that the provisions of Chapters II, III and IV apply only to contracts concluded after a data holder commits to the Data Act framework**, for example by adhering to a recognised code of conduct. Forcing the renegotiation of thousands of valid and often complex agreements, particularly in business-to-business and industrial contexts, would impose disproportionate costs and legal ambiguity.

Radically simplify governance

- Designate a single competent authority per Member State. This authority should handle all administrative functions under the DGA, including support to public sector bodies, notifications from intermediation services and registration of data altruism organisations.

[6] This issue is even more pronounced under the EHDS. Art. 52 EHDS places the full burden on the data holder to identify and justify any protections, with health data access bodies ultimately deciding whether such protections are necessary. Even in cases of serious risk of trade secret infringement, access must still be granted unless the risk 'cannot be addressed in a satisfactory manner.' The default assumption is that access should proceed even in the presence of protected intellectual assets. This sets a dangerous precedent for weakening commercial confidentiality and security, especially for sensitive health, research and industrial data. The digital package should address these shortcomings by strengthening the Data Act's protections and ensuring they apply consistently across the EHDS, where discretion to protect sensitive data should lie with the holder, not authorities. See DIGITALEUROPE, *European Health Data Space (EHDS): Key issues to address in trilogues*, available at https://cdn.digitaleurope.org/uploads/2024/01/EHDS-trilogues-DIGITALEUROPE-position-paper-1.pdf.

- Task this same authority with authorising the independent dispute resolution bodies, which should become the sole venue for resolving all disputes under the Data Act.

The governance layers created by the Data Governance Act (DGA) and the Data Act require each Member State to designate one or more competent authorities, potentially for different functions, different sectors and under different national ministries or regulators.[7] The result is institutional sprawl. Many Member States have yet to designate authorities, and those that have already struggle to coordinate roles.[8] From an industry perspective, this structure forces companies to comply with multiple interpretations, procedures and reporting lines for the very same data processing activities.

The Data Act's attempt at simplification through a 'main establishment' rule does not address the core problem: the multiplication of national regulators with unclear, untested and in some cases unnecessary mandates.

Governance must be simplified at the root. The digital package should **require each Member State to designate one single competent authority**. This authority should be tasked to handle all administrative functions under the DGA,[9] including assisting public sector bodies, receiving notifications from data intermediation services and registering data altruism organisations. This same authority should be **tasked with authorising independent dispute settlement bodies** under the Data Act. These bodies, once designated, would become the **sole forum for resolving disputes** between users, data holders, third parties and cloud service providers under the Data Act.[10]

The European Data Innovation Board should bring together the single competent authorities designated by Member States, with a mandate to develop consistent practices and advise the Commission in the exercise of its delegated powers. To ensure legitimacy and balanced input to this end, the Board should **include a broader, more representative stakeholder subgroup** to support this advisory function.

Delete overlapping data transfer rules

- Delete redundant international data transfer provisions in the Data Act, the DGA and the European Health Data Space (EHDS), which duplicate GDPR protections.

Both the Data Act and the DGA establish, in effect, a parallel framework for international data transfers that sits uneasily alongside the General Data Protection Regulation (GDPR).[11] These provisions, motivated by concerns about third-country access to EU-held data, introduce a new layer of legal uncertainty for companies operating internationally.

[7] Regulation (EU) 2022/868.

[8] https://digital-strategy.ec.europa.eu/en/news/commission-calls-10-member-states-comply-data-governance-act.

[9] Arts 7, 8, 9, 13, 14, 17, 23, 24 and 27 DGA.

[10] In addition to judicial remedy, which would always be available.

[11] Regulation (EU) 2016/679.

In addition, the EHDS introduces its own transfer rules for non-personal health datasets derived from certain personal health data categories, classifying them as 'highly sensitive' and deferring to the DGA for protective measures to be set via delegated acts.[12]

As we have consistently demonstrated, whilst these rules are framed as addressing non-personal data, they are in fact a response to scenarios that almost invariably involve personal data and are already comprehensively governed by the GDPR.[13] This is especially clear in relation to legal instruments such as the US CLOUD Act and e-evidence, which were key reference points during the legislative process.[14]

Creating overlapping regimes for data transfers is unnecessary and counterproductive. The **international transfer provisions** contained in Chapters VII Data Act and DGA, as well as those contained in Chapter V EHDS,[15] **should be deleted in full**.

Ensure practical cloud rules

- Restrict portability requirements to infrastructure services to support Europe's development of industrial solutions across sectors such as healthcare, energy, manufacturing, finance and retail.
- Allow more flexible transition periods for switching, recognising that migrations are often complex and iterative.

DIGITALEUROPE supports the objective of facilitating switching between cloud providers to promote competition and reduce vendor lock-in. However, the Data Act must be implemented in a way that avoids disproportionate burdens on providers and an unclear division of responsibility between industry and regulators.

Restrict cloud portability to infrastructure

The scope of the cloud portability provisions is overly broad, encompassing infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) under a single definition. This overlooks fundamental differences between these service models.

Unlike IaaS, which is primarily dominated by large-scale cloud infrastructure providers, SaaS and PaaS are predominantly developed and provided by companies across a wide range of sectors – including finance,

[12] Art. 88 Regulation (EU) 2025/327.

[13] See DIGITALEUROPE, *Data transfers in the Data Strategy: Understanding myth and reality*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-data-strategy_Understanding-myth-and-reality.pdf.

[14] The study underpinning the Data Act's impact assessment explicitly acknowledges that, whilst it is *theoretically* possible for non-personal data to be implicated in conflicts of law at the international level, 'in the typical scenario personal data will be involved.' Notably, the study consistently frames the issue in abstract terms and fails to provide concrete examples of non-personal data being subject to conflicting foreign legal obligations, including in relation to the US laws cited as justification for these provisions. See *Study to support an Impact Assessment on enhancing the use of data in Europe*, carried out for DG CONNECT by Deloitte, The Lisbon Council, The Joint Institute for Innovation Policy, The GovLab, Timelex and The Open Data Institute.

[15] Arts 88-89 EHDS.

healthcare, manufacturing and retail – offering specialised solutions tailored to specific industry needs. These providers are often not vertically integrated cloud platforms. By treating all these models under one portability regime, the Data Act undermines specialised digital offerings and investments by European SaaS and PaaS providers, whose services are highly integrated with customer operations and not easily transferable.

The portability requirements under Art. 30(1) and the contractual switching framework under Art. 25 jeopardise these business models by forcing providers to enable seamless switching, even when the software itself is intrinsically linked to unique configurations or custom-built environments.

This regulatory pressure has three main negative effects. First, long-term SaaS contracts, often essential for both service providers and users, would become commercially unfeasible. Second, the risk of being required to develop switching mechanisms for bespoke applications disincentivises long-term R&D and new offerings. Finally, imposing uniform switching standards risks flattening the diversity of software solutions, discouraging the creation of high-value services.

To avoid these negative outcomes, the **cloud portability provisions should be explicitly limited to infrastructure services**. These are the areas where portability is technically feasible and economically justified, as users typically require flexibility to migrate basic computing and storage resources across providers.

Simplify technical requirements for portability

Under Art. 30(1), providers of infrastructure-related services must 'facilitate the switching process' by offering not only information and documentation, but also any necessary 'capabilities,' technical support and tools – an obligation that is highly demanding.

Arts 33 and 35 allow the Commission to impose harmonised standards or common specifications, a top-down approach that overrides industry-led efforts.

To address the excessive complexity introduced by Chapter VIII, the digital package should focus on two key simplifications:

- IaaS providers should be required to **enable data and workload portability using documented, widely adopted formats**. Obligations should be limited to providing essential documentation and technical information, without requiring proprietary tools or bespoke migration support;[16] and
- The possibility for the Commission to impose **harmonised standards or common specifications should be removed**. Instead, consistent with current Art. 33(11), the Commission should issue **non-binding guidelines** where necessary, allowing standards and other industry initiatives to evolve alongside technologies and market demand.

[16] Art. 30(1) refers to 'all reasonable measures in [the providers'] power,' which could be interpreted in line with our proposed approach. The digital package should clarify this reading explicitly.

Allow flexible switching timelines

The contractual switching framework established under Art. 25 introduces fixed procedural timelines – notably a 30-day maximum transitional period and a 30-day minimum retrieval period – which are intended to facilitate customer mobility between cloud and edge service providers.

The current design is built on the assumption that switching is a linear and time-bounded operation. In practice, it is often iterative, multi-staged and contingent on third-party dependencies beyond the provider's or the customer's control. For larger customers and technically complex environments, transitions may involve phased decommissioning, compatibility assessments, security validations and data migration sequences that cannot be completed within a single 30-day window.

To reflect operational needs, the **customer should be allowed to extend the transitional period** as many times as necessary, not just once, within a reasonable limit. Additionally, **cloud providers should be permitted to extend the transitional period by up to one year**, where justified by technical complexity or security constraints, and notified within the 14-day window already foreseen in the Regulation.[17]

Consolidate a targeted public-sector data access framework

- Limit public-sector access to business data to genuine emergencies under a single, clear legal framework.
- Create a fully harmonised EU-wide system to allow businesses to access and reuse all public-sector data under consistent conditions.

Europe's regulatory landscape governing data access between the public and private sectors has become increasingly unpredictable for businesses. Rules affecting both business-to-government (B2G) data sharing and government-to-business (G2B) data reuse are spread across the Data Act, the DGA, the Open Data Directive and the revised European Statistics Regulation.[18] Each imposes different obligations, scopes and procedures, leading to duplication and inconsistencies across Member States.

A clear example is Art. 15(1)(b) Data Act, which weakens the principle of 'exceptional need' by allowing public bodies to request business data for broadly defined circumstances. This conflicts with a proportional B2G framework and risks normalising routine data requests. Similarly, Arts 17b–17e of the revised European Statistics Regulation introduce a broad second route for public access to business data for statistical purposes. Finally, Art. 21 Data Act allows public sector bodies, the Commission and the European Central Bank or a Union body to further share data received, with practically no controls in place to prevent leaks.

[17] The notification should be accompanied by a service suspension if data integrity risks being compromised during the service migration. Another aspect to consider is that Art. 34(2) Data Act permits providers to impose egress charges only to recoup actual costs incurred. Given that such costs can vary significantly depending on the provider's network investment strategy and infrastructure model, the cost calculation methodology should remain flexible to maintain incentives to invest in high-quality, resilient infrastructure.

[18] Directive (EU) 2019/1024 and Regulation (EC) No 223/2009, as amended by Regulations (EU) 2015/759 and 2024/3018, respectively.

These three provisions should be deleted to ensure that B2G access remains tightly limited to genuine public emergencies under one targeted instrument.

At the same time, the EU's G2B data reuse framework remains underexploited. Despite the Open Data Directive existing since 2003, awareness amongst companies remains low, and access is frequently undermined by fragmented national implementation, restrictive formats, poor documentation, high access fees and uneven dataset availability. To realise the potential of publicly held data for economic innovation, the Open Data Directive must be expanded to cover all public-sector data and fully harmonised, creating an EU-wide framework for businesses to access and build upon similar data under consistent conditions.

As part of this effort, Chapter II DGA should be integrated into the reformed open data framework, preserving the applicable safeguards whilst removing artificial barriers between 'open' and 'non-open' public data regimes. This would greatly strengthen trust in public data access channels and support the goal of building a single European data market.

Clarify the GDPR without reopening it

- Reinforce the use of 'legitimate interest' as a ground to process personal data for key use cases such as product development – including of AI models – and security.
- Clarify that pseudonymised data is not personal data when recipients cannot reasonably re-identify individuals.

The GDPR remains a cornerstone of European digital legislation, and a global benchmark. Its principles continue to provide a strong and future-proof foundation for personal data governance, and the protection of Europeans' fundamental rights more broadly. As such, DIGITALEUROPE does not support any reopening of the GDPR's core provisions, as this would upset the regulatory stability that has underpinned data protection in the EU and beyond since 2018.

However, several years into its implementation, certain interpretation and enforcement issues have emerged.[19] These issues, whilst not structural flaws in the GDPR itself, have created diverging national practices and unnecessary barriers to innovation. The digital package presents an opportunity to address these concerns through targeted clarifications, without undermining the GDPR's foundational logic.

Enable legitimate interest for innovation and security

Legitimate interest is intended to allow data controllers to process personal data where necessary for their legitimate purposes, if data subjects' rights and freedoms are not overridden.[20] In practice, however, the application of this legal basis has become uncertain, or even actively disfavoured by data protection authorities.

[19] See DIGITALEUROPE, *The GDPR six years in: from harmonisation to alignment*, available at https://cdn.digitaleurope.org/uploads/2024/02/The-GDPR-six-years-in-from-harmonisation-to-alignment.pdf.

[20] Art. 6(1)(f) GDPR.

In the context of AI development, for example, the European Data Protection Board (EDPB) has limited itself to stating that the lawful basis for processing personal data during the training of AI models must be determined on a case-by-case basis.[21] This won't help developers, especially where consent is impractical and contractual necessity is unavailable. As a result, lawful model training faces barriers, even where processing is low-risk and appropriately safeguarded through techniques such as pseudonymisation.[22]

Similarly, although the GDPR explicitly recognises security as an application of legitimate interest, there is often an excessively high bar for relying on it.[23] For example, controllers are expected to demonstrate prior incidents or detailed local statistics to justify even basic security measures, such as installing cameras to prevent theft or vandalism.[24] This undermines the GDPR's risk-based and proportionate spirit, and creates legal uncertainty for routine practices to protect property and assets.

We therefore recommend a targeted clarification to ensure that **legitimate interest can be confidently relied upon** where data is processed with appropriate safeguards, particularly for:

- **Product and service development and testing**, including of AI models; and
- **Security and cybersecurity measures**, including fraud prevention.

Where appropriate safeguards are in place – such as pseudonymisation where feasible, restricting access through role-based controls or setting predefined retention periods – data controllers should not be required to carry out complex balancing tests, unless there are specific indications of elevated risk to data subjects. This clarification would help align legal interpretation across Member States and ensure proportional enforcement.[25]

Apply risk-based approach to pseudonymisation and anonymisation

Pseudonymisation and anonymisation are indispensable privacy-preserving techniques used across AI development, research and data-sharing collaborations. Yet, the GDPR references anonymisation only in recitals,[26] and the treatment of pseudonymised data has been subject to diverging interpretations. Recent

[21] Opinion 28/2024.

[22] Similarly, in Guidelines 1/2024 the Board avoids clear, outcome-oriented guidance even for well-recognised use cases like product improvement. Instead, it places heavy emphasis on multilayered balancing tests and high thresholds for necessity and proportionality, even when safeguards like pseudonymisation are in place.

[23] Recital 47 GDPR explicitly recognises the prevention of fraud and ensuring network and information security as legitimate interests.

[24] Guidelines 3/2019. See DIGITALEUROPE, *Response to EDPB consultation on video devices*, available at https://cdn.digitaleurope.org/uploads/2019/09/DIGITALEUROPE-response-to-EDPB-consultation-on-video-devices.pdf.

[25] Another area requiring clarification is the interplay between the EHDS and the GDPR in identifying the correct legal basis for secondary use of personal health data. Whilst Recital 52 EHDS refers to legitimate interest as a possible legal basis, in practice companies struggle to rely on it due to uncertainty around how it interacts with the stricter requirements of Art. 9 GDPR, which governs special categories of personal data including health data). The digital package could clarify that legitimate interest can serve as a valid legal basis for secondary use, combined with the exception in Art. 9(2)(i) GDPR, which allows processing for reasons of public interest in public health. The EHDS introduces robust safeguards – including trusted governance via health data access bodies, secure processing environments and permit-based controls – that support this interpretation.

[26] Recitals 26, 28 and 29 GDPR.

draft EDPB guidelines suggest that pseudonymised data always qualifies as personal data, regardless of the context or risk of re-identification, a position that imposes unnecessary burdens on low-risk data use cases.[27]

A recent legal development strongly supports a more risk-based interpretation. In February 2025, the Advocate General of the Court of Justice of the EU concluded that pseudonymised data should not be considered personal data in the hands of a recipient who has no reasonable means to re-identify the data subjects.[28] Where the risk of re-identification is 'non-existent or insignificant,' the data in question falls outside the scope of personal data for the recipient. This position is more consistent with the GDPR's risk-based philosophy and offers a sound basis for legal clarification.

We recommend:

- Clarifying that **pseudonymised data may be considered non-personal data for third-party recipients** who have no access to, or legal means of obtaining, the re-identifying information; and
- Recognising **privacy-enhancing technologies as appropriate safeguards** that can reduce the compliance burden.

Such clarifications would remove unjustified friction, particularly for organisations pursuing valuable purposes such as research and innovation, where safeguards are in place.

FOR MORE INFORMATION, PLEASE CONTACT:

Béatrice Ericson

Manager for Data Economy, Privacy & Public Administration

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

Julien Chasserieau

Associate Director for AI & Data Policy

julien.chasserieau@digitaleurope.org / +32 492 27 13 32

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[27] Draft Guidelines 01/2025. See DIGITALEUROPE, *Pseudonymisation: a recognised tool to protect data processing*, available at https://cdn.digitaleurope.org/uploads/2025/03/Pseudonymisation-DIGITALEUROPE-0325.pdf.

[28] Opinion in Case C-413/23 P.

DIGITALEUROPE

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20